UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/934,477	08/23/2001	Sung-Kyun Park	P-218	8429

34610 7590 08/30/2006

FLESHNER & KIM, LLP
P.O. BOX 221200
CHANTILLY, VA 20153

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 08/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/934,477	PARK, SUNG-KYUN	
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20,22 and 23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *20,22 and 23* is/are allowed.

6)☒ Claim(s) *1-9,11,13 and 15-17* is/are rejected.

7)☒ Claim(s) *10, 12, 14-15, 18-19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 and 22-23 are pending.

Response to Arguments

2. Applicant's arguments have been considered but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-8, 13, and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. With regards to claims 1-8, Claim 1 provides a verifying step of "verifying the access-request message." It is unclear how the access-request message could be verified. It is the **final** access request message that contains the message digest that may be verified. Examiner suggests an amendment to clarify that it is the final access-request message being verified.

5. In addition, Claim 1 is incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. As currently presented,

AAA server would be unable to verify the final access-request message because no limitations in claim 1 provide that the AAA server has knowledge of the prescribed value. Thus, Examiner suggests an amendment to clarify that the prescribed value is known to both the AAA server and the entity requesting access similar to the limitations provided in claim 2.

6. With regards to claim 4, the determining step verifies the "authenticator value," however it is unclear which authenticator value is being identified. Examiner has interpreted the determining step to be directed to the temporarily stored value of the authenticator field as provided in claim 3. Appropriate correction or clarification is required.

7. With regards to claims 8, the claim defines that a randomly generated authenticator value. There is no antecedent basis for this limitation. Examiner suggests an amendment to follow the limitation of claim 1 defining a temporary randomly generated authenticator value. Further, the claim states that the temporary randomly generated authenticator value is created different every time. It is unclear to the Examiner if the intended meaning is that a different method of generating random numbers is used each time or that a different random number is used each time. A true random number may repeat because any number within the set of possible numbers has an equal probability of being selected. Thus, if the intended meaning of the claim is that a different random number be used each time then the intended meaning conflicts with the definition of a random number.

8. With regards to claim 13, it is unclear to the Examiner if the intended meaning is that a different method of generating an arbitrary value is used each time or that a different arbitrary value is used each time.

9. With regards to claim 15, the cited claim provides a limitation directed to "the temporary authentication value." There is no antecedent basis for this limitation. Examiner suggests a correction to read temporary authenticator value.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 9 and 16 are rejected under 35 U.S.C. 102(b) as being unpatentable over Friedman "Shared Secret Recovery in RADIUS."

11. With regards to claim 9, Friedman teaches the writing of an authenticator value for authenticating an access-request message in an authenticator field of an access-request message and transmitting an access request message (Friedman, page 3), verifying the access-request message by using the authenticator value of the access-request message when the access-request message is received (Friedman, pages 2-3), processing the access-request message if the access-request message is successfully verified (Friedman, pages 2-3), and performing user authentication by decrypting an

encrypted user password of the processed access-request message using a temporary authenticator value of the processed access-request message and a shared secret key that is known to each of a message transmitter and a message receiver (Friedman, page 3).

12. With regards to claims 16, Friedman teaches the prescribed value is a value previously defined between a foreign agent and the AAA server (Friedman, page 1, AAA server is part of Radius Protocol RFC 2138).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claim 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Friedman "Shared Secret Recovery in RADIUS" in view of West et al US Patent No. 6,538,996.

15. With regards to claims 17, Friedman teaches writing a temporary randomly generated authenticator value in an attribute field of an access-request message (Friedman, pages 2-3, pseudo-random bit request), encrypting a user password using

the temporary authenticator value (Friedman, page 2), transmitting the final access request message to an Authentication, Authorization, and Accounting server (Friedman, pages 1-3), and verifying the access-request message by the AAA server (Friedman, page 3, yield original password). Friedman fails to teach the executing of an encryption algorithm to generate a message digest and the filling of fields of a request message. West teaches executing an encryption algorithm using the access request message having the temporary authenticator value and the user password to generate a message digest (West, column 28 lines 25-29, hash of random and password), the access request message having an authenticator field that is filled with a prescribed value, generating a final access-request message, the final-access request message being generated by using the access request message (West, column 28 lines 25-33, generates using password and random) and replacing the value of the authenticator field with the message digest (West, column 28 lines 25-33, authenticator field filled with random number, replaces value with hash value, random discarded). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize West's method of creating message digests with Friedman's disclosure because it offers the advantage of allowing a method of authenticating messages between a client and accounting server without sending a password in the clear (West, column 28 lines 25-33).

16. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Friedman "Shared Secret Recovery in RADIUS" in view of Morgan et al US Patent No. 6,088,799.

17. With regards to claim 11, Friedman teaches an encrypted user password written in an attribute field of an access-request message (Friedman, page 3), but fails to teach the decrypting of the user password and comparison with a stored user password. Morgan teaches decrypting the user password (Morgan, column 7 line 66 – column 8 line 16), comparing the decrypted user password and a user password stored in a database (Morgan, column 8 lines 4-7), determining that the user authentication is successful if the decrypted password and the stored user password are identical to each other and determining that the user authentication has failed if the decrypted user password and the stored user password are not identical to each other (Morgan, column 8 lines 7-16). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Morgan's password checking system with Friedman's disclosure because it offers the advantage of ensuring that only authenticated user's gain access to sensitive data such as encryption keys (Morgan, column 3 line 65 – column 4 line 7).

Allowable Subject Matter

18. Claims 1-8 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

19. Claims 10, 12, 14, and 18-19 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

20. Claims 13 and 15 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and if they are rewritten in independent form including all of the limitations of the base claim and any intervening claims.

21. Claims 20 and 22-23 are allowed.

22. The following is a statement of reasons for the indication of allowable subject matter:

23. With regards to claims 1-8 and 18, the cited claims provide limitations requiring generating a final access request message where the final access request message is generated by using the access-request message and replacing the value of the authenticator field by the message digest. The cited prior art fails to specifically teach or suggest the steps generating a final access request message where the final access request message is generated by using the access-request message and replacing the value of the authenticator field by the message digest as defined in the cited claim. Thus the cited prior art fails to anticipate or render obvious the above-cited claims.

24. With regards to claims 10, 19-20, and 23, the cited claims provide limitations requiring "temporarily storing the contents of the authenticator field of the access-request message; filling the authenticator field with the prescribed value; performing an encrypting algorithm to obtain a message digest; and verifying the access-request

message by comparing the temporarily stored authenticator value to the message digest." The cited prior art fails to specifically teach or suggest the steps of temporarily storing the contents of the authenticator field, re-filling the authenticator field with the prescribed value, and obtaining a message digest as defined in the cited claim. Thus the cited prior art fails to anticipate or render obvious the above-cited claims.

25. With regards to claims 12-15, the cited claims provide limitations requiring "creating the authenticator value for authentication of the access-request message using the temporary authenticator value and a prescribed value previously defined between the message transmitter and the message receiver; and writing the authenticator value in the authenticator field and generating the access-request message." The cited prior art fails to specifically teach or suggest the steps of creating the authenticator value for authentication of the access-request message using the temporary authenticator value and a prescribed value previously defined between the message transmitter and the message receiver; and writing the authenticator value in the authenticator field and generating the access-request message as defined in the cited claim. Thus the cited prior art fails to anticipate or render obvious the above-cited claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272

3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571 272 6962. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven
AN

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100